

#3  
5-14-02  
SM

S&H Form: (2/01)

Attorney Docket No. 1083.1083

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

Hisao NAITOH

Application No.:

Group Art Unit:

Filed: July 12, 2001

Examiner:

For: COMPUTER VIRUS INFECTION INFORMATION PROVIDING METHOD, COMPUTER VIRUS INFECTION INFORMATION PROVIDING SYSTEM, INFECTION INFORMATION PROVIDING APPARATUS, AND COMPUTER MEMORY PRODUCT

JC997 U.S. PTO  
09/902583  
07/12/01

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2001-088710

Filed: March 26, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: July 12, 2001

By: \_\_\_\_\_

James D. Halsey, Jr.  
Registration No. 22,729

700 11th Street, N.W., Ste. 500  
Washington, D.C. 20001  
(202) 434-1500

©2001 Staas & Halsey LLP

PATENT OFFICE  
JAPANESE GOVERNMENT

JC997 U.S. PTO  
09/902583  
07/12/01

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: March 26, 2001  
Application Number: Patent Application No. 2001-088710  
Applicant (s): FUJITSU LIMITED

May 11, 2001  
Commissioner, Japanese Patent Office  
Kozo OIKAWA

Patent application 2001-088710

[Name of Document]	Patent Application
[Reference Number]	0095402
[Date of Filing]	March 26, 2001
[Destination]	Commissioner, Patent Office
[International Patent Classification]	G06F 11/30
[Title of Invention]	COMPUTER VIRUS INFECTION INFORMATION PROVIDING METHOD AND COMPUTER VIRUS INFECTION INFORMATION PROVIDING SYSTEM
[Number of Claimed Inventions]	5
[Inventor]	
[Address]	c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa
[Name]	Hisao NAITOH
[Applicant]	
[Identification Number]	000005223
[Name]	FUJITSU LIMITED
[Attorney]	
[Identification Number]	100078868
[Patent Attorney]	
[Name]	Takao KOHNO
[Telephone Number]	06-6944-4141
[Indication of Official Fee]	
[Register Number]	001889
[Amount]	¥21,000
[List of Annexes]	
[Name of Article]	Specification 1
[Name of Article]	Drawings 1
[Name of Article]	Abstract 1
[Number of General Authorization]	9705356
[Proof]	Needed

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

JC997 U.S. P1  
09/902583  
07/12/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office

出 願 年 月 日

Date of Application:

2001年 3月26日

出 願 番 号

Application Number:

特願2001-088710

出 願 人

Applicant(s):

富士通株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 5月11日

特許庁長官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3040490

【書類名】 特許願

【整理番号】 0095402

【提出日】 平成13年 3月26日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 11/30

【発明の名称】 コンピュータウィルス感染情報提供方法及びコンピュータウィルス感染情報提供システム

【請求項の数】 5

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 内藤 久生

【特許出願人】

    【識別番号】 000005223

    【氏名又は名称】 富士通株式会社

【代理人】

    【識別番号】 100078868

    【弁理士】

    【氏名又は名称】 河野 登夫

    【電話番号】 06-6944-4141

【手数料の表示】

    【予納台帳番号】 001889

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9705356

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンピュータウイルス感染情報提供方法及びコンピュータウイルス感染情報提供システム

【特許請求の範囲】

【請求項 1】 端末装置と中央装置との間で送受信される情報に、コンピュータウイルスが存在するか否かを検出し、検出したコンピュータウイルスに関する感染情報を提供するコンピュータウイルス感染情報提供方法において、

前記中央装置に、コンピュータウイルスを検出及び駆除するワクチンを登録し、また前記端末装置の通信履歴を記憶しておき、前記登録したワクチンにより、前記コンピュータウイルスが検出された場合に、前記記憶した通信履歴に基づいて、感染時期を特定し、

該特定した感染時期を含む感染情報を前記中央装置から前記端末装置へ送信し

前記端末装置により、前記送信された感染情報を表示する

ことを特徴とするコンピュータウイルス感染情報提供方法。

【請求項 2】 端末装置と中央装置との間で送受信される情報に、コンピュータウイルスが存在するか否かを検出し、検出したコンピュータウイルスに関する感染情報を提供するコンピュータウイルス感染情報提供システムにおいて、

前記中央装置は、

コンピュータウイルスを検出及び駆除するワクチンを登録する手段と、

前記端末装置の通信履歴を記憶する手段と、

前記登録したワクチンにより、前記コンピュータウイルスが検出された場合に、前記記憶した通信履歴に基づいて、感染時期を特定する特定手段と、

前記特定した感染時期を含む感染情報を前記端末装置へ送信する感染情報送信手段と

を備え、

前記端末装置は、

前記送信された感染情報を表示する手段

を備えることを特徴とするコンピュータウイルス感染情報提供システム。

【請求項 3】 前記中央装置は、  
前記コンピュータウィルスが発見された発見日時を登録する手段  
を更に備え、  
前記特定手段は、  
前記登録したワクチンにより、前記コンピュータウィルスが検出された場合に  
、前記記憶した通信履歴、前記登録した発見日時、及び前記ワクチンを登録した  
ワクチン登録日時に基づいて、感染時期を特定するよう構成してある  
ことを特徴とする請求項 2 に記載のコンピュータウィルス感染情報提供システ  
ム。

【請求項 4】 前記中央装置は、  
前記記憶した通信履歴及び前記ワクチンを登録した登録日時に基づいて前記コ  
ンピュータウィルスの感染経路を特定する経路特定手段  
を更に備え、  
前記感染情報送信手段は、  
前記特定した感染経路、及び前記特定した感染時期を含む感染情報を前記端末  
装置へ送信するよう構成してあることを特徴とする請求項 2 または 3 に記載のコ  
ンピュータウィルス感染情報提供システム。

【請求項 5】 前記中央装置は、  
前記登録したワクチンを予め指定された端末装置へ送信する手段  
を更に備え、  
前記端末装置は、  
前記送信されたワクチンを登録する手段と、  
該登録したワクチンの実行履歴を記憶する手段と、  
前記ワクチンにより、前記コンピュータウィルスが検出された場合に、前記記  
憶した実行履歴を前記中央装置へ送信する実行結果送信手段  
を更に備え、  
前記中央装置は、  
前記実行結果送信手段により送信された実行履歴及び前記登録した発見日時に  
基づいて感染時期を特定する補助特定手段と、

前記実行結果送信手段により送信された実行履歴に基づいて、前記コンピュータウィルスの感染経路を特定する補助経路特定手段と、

前記補助特定手段により特定した感染時期、及び前記補助経路特定手段により特定した感染経路を含む感染情報を前記端末装置へ送信する手段と

を更に備えることを特徴とする請求項3または4に記載のコンピュータウィルス感染情報提供システム。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、端末装置と中央装置との間で送受信される情報に、コンピュータウィルスが存在するか否かを検出し、検出したコンピュータウィルスに関する感染情報を提供するコンピュータウィルス感染情報提供方法及びコンピュータウィルス感染情報提供システムに関し、特に感染情報として感染時期及び感染経路を提供し、ユーザの端末装置に、コンピュータウィルスがどのようにして感染したかの情報を提供するコンピュータウィルス感染情報提供方法、及びコンピュータウィルス感染情報提供システムに関する。

##### 【0002】

#### 【従来の技術】

近年、インターネットまたはフロッピーディスク等の記録媒体から、コンピュータに侵入し、コンピュータの正常な動作を意図的に妨げるコンピュータウィルスが蔓延している。これらのコンピュータウィルスは、感染したコンピュータのみならず、他のコンピュータにも感染する虞があることから、新種のコンピュータウィルスの発見後は速やかに、コンピュータウィルスを検出及び駆除するワクチンが作成され、ユーザに配布される。

##### 【0003】

係るワクチンは、一般にユーザの端末装置にインストールされ、端末装置が一定期間毎にまたはファイル操作時にウィルスチェックを実行することにより、コンピュータウィルスを検出する。また、近年インターネットを経由する電子メールにコンピュータウィルスを添付ファイルとして、第3者に無差別に送りつける



タイプも存在することから、インターネットサービスプロバイダ（以下、ISPという）の中央装置内にワクチンをインストールしておき、当該ISPを経由するファイルを逐次ウイルスチェックすることにより、未然に感染を防止する試みがなされている。

【0004】

【発明が解決しようとする課題】

しかしながら、ISPにおける中央装置において、コンピュータウイルスが検出された場合でも、単に検出された旨が通知されるのみであり、ユーザにとっては何時、何処からコンピュータウイルスが侵入したのか分からないという問題があった。特に、インターネット経由で感染するケースが増加していることに鑑みれば、詳細な感染情報をユーザに提供することが望まれる。

【0005】

また、ワクチンはISPにおける中央装置のみならず、ユーザの端末装置にも常に最新のワクチンをインストールしておくことが、効果的である。しかし、ユーザはワクチン製作会社が製作したワクチンをインストール後は、最新のワクチンにアップロードすることが少なく、効果的にコンピュータウイルスを除去することができていないという問題があった。さらに、ワクチンの製作は多大な費用を要するにも拘わらず、ユーザは一度ワクチンを入手した後は、わざわざ対価を支払って最新のワクチンを入手する体制にないため、ワクチン製作会社の収益の悪化をも招いていた。

【0006】

つまり、他のISPとの差別化を図るべくISPにおいて、よりコンピュータウイルスに関する詳細な感染情報を提供することにより、ISPの付加価値を高め、また最新のワクチンを各ユーザに配布して、ワクチン製作に要する対価を回収することが可能なシステムの構築が要請されていた。

【0007】

本発明は斯かる事情に鑑みてなされたものであり、その目的とするところは中央装置においてユーザの端末装置の通信履歴を監視し、感染時期等の感染情報をユーザに提供することにより、容易にユーザが感染時期を把握することができ、

またこれにより I S P の付加価値を高めることが可能なコンピュータウィルス感染情報提供方法、及びコンピュータウィルス感染情報提供システムを提供することにある。

【 0 0 0 8 】

また、本発明の他の目的は、コンピュータウィルスの発見日時及びワクチンの登録日時をも考慮することにより、より精度良く感染時期を特定することが可能なコンピュータウィルス感染情報提供システムを提供することにある。

【 0 0 0 9 】

また、本発明の他の目的は、コンピュータウィルスの感染経路をも提供することにより、さらにコンピュータウィルスの感染原因を判断することが容易となるコンピュータウィルス感染情報提供システムを提供することにある。

【 0 0 1 0 】

さらに、本発明の他の目的は、ワクチンを予め指定したユーザにのみ配布し、また端末装置においてもコンピュータウィルスチェックを行いその結果に基づいて、感染時期を特定し感染情報としてユーザに提供することにより、感染時期の精度を向上させることができ、またワクチン製作に要する対価を確実に回収することが可能なコンピュータウィルス感染情報提供システムを提供することにある。

【 0 0 1 1 】

【課題を解決するための手段】

第 1 発明に係るコンピュータウィルス感染情報提供方法は、端末装置と中央装置との間で送受信される情報に、コンピュータウィルスが存在するか否かを検出し、検出したコンピュータウィルスに関する感染情報を提供するコンピュータウィルス感染情報提供方法において、前記中央装置に、コンピュータウィルスを検出及び駆除するワクチンを登録し、また前記端末装置の通信履歴を記憶しておき、前記登録したワクチンにより、前記コンピュータウィルスが検出された場合に、前記記憶した通信履歴に基づいて、感染時期を特定し、該特定した感染時期を含む感染情報を前記中央装置から前記端末装置へ送信し、前記端末装置により、前記送信された感染情報を表示することを特徴とする。

## 【0012】

第2発明に係るコンピュータウイルス感染情報提供システムは、端末装置と中央装置との間で送受信される情報に、コンピュータウイルスが存在するか否かを検出し、検出したコンピュータウイルスに関する感染情報を提供するコンピュータウイルス感染情報提供システムにおいて、前記中央装置は、コンピュータウイルスを検出及び駆除するワクチンを登録する手段と、前記端末装置の通信履歴を記憶する手段と、前記登録したワクチンにより、前記コンピュータウイルスが検出された場合に、前記記憶した通信履歴に基づいて、感染時期を特定する特定手段と、前記特定した感染時期を含む感染情報を前記端末装置へ送信する感染情報送信手段とを備え、前記端末装置は、前記送信された感染情報を表示する手段を備えることを特徴とする。

## 【0013】

第3発明に係るコンピュータウイルス感染情報提供システムは、第2発明において、前記中央装置は、前記コンピュータウイルスが発見された発見日時を登録する手段を更に備え、前記特定手段は、前記登録したワクチンにより、前記コンピュータウイルスが検出された場合に、前記記憶した通信履歴、前記登録した発見日時、及び前記ワクチンを登録したワクチン登録日時に基づいて、感染時期を特定するよう構成してあることを特徴とする。

## 【0014】

第4発明に係るコンピュータウイルス感染情報提供システムは、第2発明または第3発明において、前記中央装置は、前記記憶した通信履歴及び前記ワクチンを登録した登録日時に基づいて前記コンピュータウイルスの感染経路を特定する経路特定手段を更に備え、前記感染情報送信手段は、前記特定した感染経路、及び前記特定した感染時期を含む感染情報を前記端末装置へ送信するよう構成してあることを特徴とする。

## 【0015】

第5発明に係るコンピュータウイルス感染情報提供システムは、第3発明または第4発明において、前記中央装置は、前記登録したワクチンを予め指定された端末装置へ送信する手段を更に備え、前記端末装置は、前記送信されたワクチン

を登録する手段と、該登録したワクチンの実行履歴を記憶する手段と、前記ワクチンにより、前記コンピュータウイルスが検出された場合に、前記記憶した実行履歴を前記中央装置へ送信する実行結果送信手段を更に備え、前記中央装置は、前記実行結果送信手段により送信された実行履歴及び前記登録した発見日時に基づいて感染時期を特定する補助特定手段と、前記実行結果送信手段により送信された実行履歴に基づいて、前記コンピュータウイルスの感染経路を特定する補助経路特定手段と、前記補助特定手段により特定した感染時期、及び前記補助経路特定手段により特定した感染経路を含む感染情報を前記端末装置へ送信する手段とを更に備えることを特徴とする。

## 【 0 0 1 6 】

第1発明及び第2発明にあつては、中央装置にコンピュータウイルスを検出及び駆除するワクチンを登録しておく。また、中央装置は通信網を介して接続される端末装置が送信する情報の通信履歴を記憶する。そして、登録したワクチンにより、送信される情報中にコンピュータウイルスが検出された場合、記憶した通信履歴に基づいて、感染時期を特定する。例えば、通信履歴として、情報を送信した日時を記憶しておき、前回端末装置が情報を送信した日時にコンピュータウイルスが検出されず、今回情報を送信した日時にコンピュータウイルスが検出された場合、前回情報を送信した日時から今回情報を送信した日時の間に、他のISP経由または記録媒体経由で感染したことが特定できる。そして、この特定した感染時期を含む感染情報を前記端末装置へ送信する。送信する内容としては感染時期、感染したコンピュータウイルス名等である。

## 【 0 0 1 7 】

そして、前記端末装置は、送信された感染時期を含む感染情報を表示するようにしたので、ユーザはより詳細なコンピュータウイルスの情報を入手でき、感染原因を特定することが容易となる。特に、係る詳細な感染情報を提供することで、他のISPとの差別化を図り、ISPの付加価値を飛躍的に高めることが可能となる。

## 【 0 0 1 8 】

第3発明にあつては、感染時期の特定に当たって、さらに、ワクチン製作会社

、またはISPがコンピュータウィルスを最初に発見した日時を考慮する。すなわち、コンピュータウィルスは最初に発見されてから次第に蔓延していく性質を有することから、コンピュータウィルスが最初に発見される以前に、ユーザの端末装置がコンピュータウィルスに感染している場合は、極めて稀である。換言すれば感染時期が発見日時以前である可能性は極めて低い。

## 【0019】

また、感染時期の特定に当たって、さらに、発見されたコンピュータウィルスに対するワクチンを中央装置に登録した日時を考慮する。つまり、中央装置にワクチンを登録した登録日時以降は、完全に中央装置を経由するコンピュータウィルスはブロックすることが可能である。従って、コンピュータウィルスが検出された場合、前回の情報送信日時がワクチン登録日時以降であるか否かによって、感染時期が大きく異なる。前回の情報送信時がワクチン登録日時以降である場合は、前回はコンピュータウィルスに感染していることはあり得ないことから、前回情報を送信した日時から今回情報を送信した日時の間に、他のISP経由または記録媒体経由で感染したことが特定できる。一方、今回情報を送信し、コンピュータウィルスが検出された場合に、前回情報を送信した日時が、ワクチン登録日時以前である場合は、感染時期はそれ以前の発見日時から今回情報を送信した日時の間であることが特定できる。以上のように、感染時期を詳細に決定すべく判断要素として通信履歴に加えて、コンピュータウィルスの発見日時及びワクチン登録日時をも加えるようにしたので、より精度良く感染時期を特定でき、ユーザが感染原因を特定することがさらに容易になる。

## 【0020】

第4発明にあっては、記憶した通信履歴及びワクチンを登録した登録日時に基づいてコンピュータウィルスの感染経路を特定する。つまり、ワクチンを中央装置にインストールした後（登録日時の後）に、前回端末装置から情報を送信した場合にコンピュータウィルスが検出されず、今回情報を送信した場合に、コンピュータウィルスが検出されたということは、端末装置は明らかに中央装置（当該ISP）経由で感染したという可能性が無くなる。一方、ワクチンを中央装置にインストールした後（登録日時の後）に、今回情報を送信した場合に、コンピュ

ータウィルスが検出され、かつ前回情報を送信した日時が登録日時以前である場合は、登録日時以前に中央装置（当該ISP）を経由した可能性を否定できない。このように、通信履歴及びワクチンの登録日時に基づいてコンピュータウィルスの感染経路を特定し、感染経路をも感染情報としてユーザに提供することとしたので、ユーザはより感染経路を特定することが容易になる。

#### 【0021】

第5発明にあっては、登録したワクチンを中央装置から予め指定された端末装置のみへ送信する。ワクチンが送信された端末装置は、ワクチンを登録する。そして、一定期間毎に、またはファイル操作時等に実行されるワクチンの実行履歴を記憶しておく。そして、ワクチンにより、コンピュータウィルスが検出された場合、前記記憶した実行履歴を中央装置へ送信する。

#### 【0022】

中央装置は、実行履歴及び前記登録した発見日時に基づいて感染時期を特定する。また、送信された実行履歴に基づいて、コンピュータウィルスの感染経路を特定する。つまり上述した方法と同じく、ローカルな端末装置においてもウィルスチェックを行い、その実行履歴等の情報を回収し、これらに基づいて感染時期及び感染経路を特定して、ユーザへ提供する。従って、予め最新のワクチンの提供を受けるべくライセンス契約を行っているユーザは、新たなコンピュータウィルスの感染を防止することができる。また、ローカルな端末装置でのコンピュータウィルスチェックの結果に基づいて感染時期を特定しているので、さらに詳細に感染時期及び感染経路を特定することが可能となる。さらに、ISPの各ユーザから、ライセンス契約によりワクチンの製作に対する対価を確実に回収できることから、コンピュータウィルスの発生度に、定期的な収入が見込め、ワクチン製作会社の経営基盤を盤石のものとすることが可能となる。

#### 【0023】

##### 【発明の実施の形態】

以下本発明を実施の形態を示す図面に基づいて詳述する。

##### 実施の形態1

図1は本発明に係るコンピュータウィルス感染情報提供システムの概要を示す

模式図である。図において1はインターネットの接続サービスを提供するISP等の中央装置であり、インターネット等の通信網Nを介してパーソナルコンピュータまたは携帯端末装置等の端末装置2, 2, 2...と接続されている。端末装置2はISPとの間で、契約することにより、ログイン名及び電子メールアドレス等が与えられ、所定のアクセスポイントにアクセスすることにより、中央装置1を経由して、ネットサーフィン及び電子メールの送受信が可能となる。なお、本実施の形態においてはISPにおける中央装置1と各家庭のパーソナルコンピュータ等の端末装置2とがインターネットにより接続されているシステムについて説明するが、これに限らず、企業等のLAN(Local Area Network)におけるサーバコンピュータ等の中央装置1と、クライアントコンピュータ等の端末装置2との間におけるシステム等であっても良い。

## 【0024】

図2は中央装置1の構成を示すブロック図である。図に示すように、CPU11にはバス17を介してRAM12, ハードディスク等の記憶部15、端末装置2と情報を送受信するためのゲートウェイ等の通信部16、液晶ディスプレイ等の表示部13、及びキーボード、マウス等の入力部14が接続される。RAM12には記憶部15、表示部13、及び入力部14等を制御するための制御プログラム12Pが記憶されている。記憶部15には、製作されたワクチンを登録したワクチン登録ファイル151, 端末装置2の通信履歴を記憶する通信履歴記憶ファイル152, 及びユーザのログイン名、電子メールアドレス等を記憶したユーザファイル153が設けられている。なお、ワクチン登録ファイル151, 通信履歴記憶ファイル152, 及びユーザファイル153は必ずしも中央装置1の記憶部15に設けられている必要はなく、通信網Nを介して接続される図示しない他のコンピュータの記憶部に設けておき、必要に応じて読み出すようにしても良い。

## 【0025】

CPU11は、端末装置2から情報が送信された場合、その通信履歴を通信履歴記憶ファイル152に記憶する。CPU11は電子メールに添付ファイルが存在し、ゲートウェイ等の通信部16をこれらのファイルが通過する場合は、ワク

チン登録ファイル 1 5 1 に登録したワクチンにより、コンピュータウィルスを検出し、駆除する。

## 【 0 0 2 6 】

図 3 はワクチン登録ファイル 1 5 1 のレコードレイアウトを示す説明図である。図に示すようにワクチンを特定するための固有のワクチンコードに対応して、コンピュータウィルスが発見された発見日時、及び該コンピュータウィルスを検出し、駆除するワクチンを登録した登録日時がそれぞれ記憶されている。なお、図示しないが、ワクチンコードに対応してワクチン登録ファイル 1 5 1 には、コンピュータウィルスを検出及び駆除するワクチンが登録されている。また、ワクチンはコンピュータウィルスが発見される度に、新たなコンピュータウィルスを検出及び駆除する機能が、従来のワクチンに対して追加される。

## 【 0 0 2 7 】

図 4 はユーザファイル 1 5 3 のレコードレイアウトを示す説明図である。図に示すように中央装置 1 へログインするために、ユーザ毎に付与される固有のログイン名に対応させて、パスワード、電子メールアドレス及び氏名等が記憶されている。

## 【 0 0 2 8 】

図 5 は通信履歴記憶ファイル 1 5 2 のレコードレイアウトを示す説明図である。図に示すように、端末装置 2、つまりユーザのログイン名毎に通信履歴が記憶されている。通信履歴は、各端末装置 2、2、2…が情報を送信した情報送信日時に対応して、対応ワクチンコード及び検出したコンピュータウィルスが記憶されている。対応ワクチンコードフィールドには、情報の送信日時に中央装置 1 にインストールされているワクチンの、ワクチンコードが記憶されている。また、ワクチンが実行され、コンピュータウィルスが検出された場合は、検出されたウィルス名が検出コンピュータウィルスフィールドに記憶される。なお、ワクチンを実行した結果、コンピュータウィルスが検出されなかった場合、検出コンピュータウィルスフィールドには、検出されなかったことを示す情報が記憶される（図の×印）。

## 【 0 0 2 9 】



図6は本発明に係るコンピュータウィルス感染情報提供システムの処理手順を示すフローチャートである。まず、新たなコンピュータウィルスが発見された場合は、それが発見された日時をワクチン登録ファイル151に登録する（ステップS61）。発見されたコンピュータウィルスを検出及び駆除するワクチンが、製作された場合、当該ワクチンを中央装置1のワクチン登録ファイル151に登録（インストール）し、またワクチンの登録日時をも該ワクチンに対応させて登録する（ステップS62）。ワクチン登録ファイル151には、図3に示すようにワクチンを特定するための固有のワクチンコードに対応させて、コンピュータウィルス発見日時、ワクチン登録日時及びワクチン（図示せず）が登録される。なお、ワクチンの製作には一定期間を要するため、コンピュータウィルス発見日時とワクチン登録日時とには、不可避免的にタイムラグが存在する。

#### 【0030】

また、中央装置1は端末装置2の通信履歴を通信履歴記憶ファイル152に記憶する（ステップS63）。具体的には図5に示すように、中央装置1は、ログイン名に対応させて、端末装置2が中央装置1へ情報を送信した日時等を記憶する。なお、通信履歴としてログイン日時、及びログアウト日時を記憶するようにしても良い。

#### 【0031】

中央装置1は、端末装置2から中央装置1を経由して情報が送信された場合は、その情報中にコンピュータウィルスが存在するか否かを、登録したワクチンにより検出し、コンピュータウィルスを検出した場合は、通信履歴等に基づいて、該端末装置2がコンピュータウィルスに感染した感染時期を特定し（ステップS64）、さらに感染経路を特定する（ステップS65）。なお、感染時期及び感染経路を特定する際の詳細な処理手順については、後述する。

#### 【0032】

中央装置1は、特定した感染時期、特定した感染経路及び検出したコンピュータウィルス名、および対処方法等のコンピュータウィルスに関する感染情報を、ユーザファイル153に登録した電子メールアドレスを参照して、端末装置2へ送信する（ステップS66）。端末装置2は、送信された感染情報を図示しない

液晶ディスプレイ等の表示部 13 に表示する（ステップ S 67）。なお、表示内容については、後述する。

#### 【0033】

図 7 は感染時期の特定処理及び感染経路の特定処理の手順を示すフローチャートである。まず、端末装置 2 が中央装置 1 を経由して送信する情報に、コンピュータウィルスが存在するか否かを検出する（ステップ S 71）。具体的には、送信されるファイル名またはファイルの内容を、ワクチン登録ファイル 151 に登録した最新のワクチンを用いて、マッチング処理等によりチェックし、そのファイルがコンピュータウィルスに該当するか否かを判断する。コンピュータウィルスが検出されない場合は（ステップ S 71 で NO）、検出されなかったことを示す情報を、通信履歴記憶ファイル 152 の検出コンピュータウィルスフィールドに記憶する（ステップ S 72）。なお、図 5 では検出コンピュータウィルスフィールドに×印を用いて示している。また、中央装置 1 はコンピュータウィルスチェックを実行したワクチンのワクチンコードを、対応ワクチンコードフィールドに記憶する。

#### 【0034】

一方、コンピュータウィルスが検出された場合は（ステップ S 71 で YES）、中央装置 1 は通信履歴記憶ファイル 152 を参照して、前回に情報を送信した日時を読み出す（ステップ S 73）。そして、図 5 に示すように今回情報を送信した日時に対応させて、検出したコンピュータウィルス名をも、検出コンピュータウィルスフィールドに記憶する。

#### 【0035】

続いて、中央装置 1 はワクチン登録ファイル 151 を参照して、ワクチン登録日時を読み出す。そして、それぞれ読み出した前回に情報を送信した日時とワクチン登録日時とを比較して、前回に情報を送信した日時がワクチン登録日時以降であるか否かを判断する（ステップ S 74）。

#### 【0036】

ここで、前回に情報を送信した日時がワクチン登録日時以降である場合は（ステップ S 74 で YES）、感染時期を前回に情報を送信した日時からコンピュー

タウィルスの検出日時である、今回に情報を送信した日時までの間と特定する（ステップS75）。さらに、感染経路を中央装置1以外（中央装置1のISP以外）と特定する（ステップS76）。

## 【0037】

つまり、ワクチンを中央装置1において登録した後は、中央装置1を備えるISPを経由するコンピュータウィルスは全てブロックされる。このような状況下で、前回に送信された情報にコンピュータウィルスが存在しないということは、前回情報送信時はコンピュータウィルスに感染していないといえる。そして、今回初めてコンピュータウィルスが検出されたということは、他のISP経由またはフロッピーディスク等の記録媒体経由で、前回に情報を送信した日時から今回に情報を送信した日時の間に感染したといえる。例えば、他のISP経由で、メーカーのアドレス帳に登録した電子メールアドレス先に、感染したコンピュータウィルスを送りつけるものに、端末装置2が感染した場合は、前回に情報を送信した際は、検出されず、今回に情報を送信した際に検出されたことから、感染経路が他のISP経由またはフロッピーディスク等の記録媒体経由であると感染経路を特定でき、さらに感染時期も少なくとも前回に情報を送信した日時から今回に情報を送信した日時の間と特定することが可能となる。

## 【0038】

一方、前回に情報を送信した日時がワクチン登録日時以降でない場合は（ステップS74でNO）、感染時期を発見日時から検出日時までの間に特定し（ステップS77）、また感染経路を中央装置1、他のISP経由または記録媒体と特定する（ステップS78）。通常このようなケースは稀であるが、ワクチンが中央装置1において登録される以前に、すなわちISPにおいてコンピュータウィルスをブロックする状態になる以前に、早期に端末装置2が感染する場合もあり得る。かかる場合、コンピュータウィルスが初めて発見される日時以前に端末装置2において感染するケースは極めて稀であることから、感染時期を発見日時から今回情報を送信した日時の間と特定する。また、感染経路についても、中央装置1を経由した可能性を否定できないことから、中央装置1、他のISPまたはフロッピーディスク等の記録媒体と特定する。

## 【0039】

以上の処理を経て、感染時期及び感染経路が特定した場合は、端末装置2へ感染情報を送信する。図8は感染情報の表示例を示す説明図である。図8に示すように特定した感染時期及び感染経路を電子メールとして送信する。この際、検出したコンピュータウィルス名、対策方法をも感染情報として提供する。

## 【0040】

## 実施の形態2

実施の形態2は予め定められた端末装置2へワクチンを提供し、その実行結果を分析することによりより詳細な感染情報を提供するものである。図9は実施の形態2に係るユーザファイル153のレコードレイアウトを示す説明図である。図9において、ワクチンの提供を受けるべく登録を受けているユーザはワクチン登録フィールドに、○印で示しており、一方、登録を受けていないユーザは×印で示している。ワクチンの提供を受けるユーザは、中央装置1を管理するISPに所定の対価を支払うことを条件に、ワクチンが更新される度に、ワクチンの提供を受けることができる。これにより、ワクチン製作者は、新たなウィルスが発見される度に、ワクチン製作に伴う費用を、ISPを経由して確実に回収することが可能となる。

## 【0041】

図10は実施の形態2に係る端末装置2の構成を示すブロック図である。実施の形態2に係る端末装置2は公知のコンピュータと同様の構成をしており、CPU21に、バス27を介してRAM22、ハードディスク等の記憶部25、中央装置1と情報を送受信するためのモデム等の通信部26、液晶ディスプレイ等の表示部24、及びキーボード、マウス等の入力部23が接続される。またRAM22には記憶部25、表示部24、及び入力部23等を制御するための制御プログラム22Pが記憶されている。

## 【0042】

記憶部25には、中央装置1からダウンロードしたワクチンが記憶されており、ワクチンはRAM22にロードされコンピュータウィルスの検出を実行する。実行結果は実行履歴ファイル251に記憶される。図11は実行履歴ファイル2

51の記録内容を示す説明図である。図に示すようにワクチンの実行日時に対応させて、検出結果、実行したワクチンコード及び検出したコンピュータウイルス名が記憶されている。検出結果フィールドにはワクチン実行日時において、コンピュータウイルスを検出した場合にフラグがたてられ（図の○印）、検出したコンピュータウイルス名が検出コンピュータウイルスフィールドに記憶される。

#### 【0043】

図12は実施の形態2に係るコンピュータウイルス感染情報提供システムの処理手順を示すフローチャートである。まず、実施の形態1と同様に新規なコンピュータウイルスに対応するワクチンを中央装置1のワクチン登録ファイル151に登録する（ステップS101）。続いて、ユーザファイル153を参照して、ユーザがワクチン登録者であるか否かを判断する（ステップS102）。ここで、ワクチン登録者である場合は（ステップS102でYES）、電子メールアドレスを参照して、登録しているユーザに係る端末装置2へ、ワクチンを送信する（ステップS104）。

#### 【0044】

一方、ワクチンの登録ユーザでない場合（ステップS102でNO）、ワクチンの提供に関する案内情報を端末装置2へ送信する（ステップS103）。案内情報としては、所定の対価を支払うことを条件に、ワクチンの提供を受けることができる旨の案内を電子メールとして図13の如く送信する。なお、案内情報の送信の際はユーザファイル153を参照して、ワクチン登録がなされていないユーザの電子メールアドレスを参照して、送信する。図13は案内情報のイメージを示す説明図である。図に示すような案内情報が送信される。また図に示すようにワクチン登録をするためのWebページへジャンプするハイパーリンクを送信するようにしても良い。これにより、ワクチン登録をしていないユーザへ注意を喚起することができ、ワクチン登録者を増加することが可能となる。

#### 【0045】

ワクチンを受信した端末装置2は記憶部25にワクチンを登録する（ステップS105）。そして、端末装置2はワクチンが実行される度に実行履歴を実行履歴ファイル251に記憶し（ステップS106）、実行した場合、コンピュータ

ウイルスが検出されたか否かを判断する（ステップS107）。そして、コンピュータウイルスが発見された場合は（ステップS107でYES）、実行履歴ファイル251を読み出して中央装置1へ送信する（ステップS108）。一方、コンピュータウイルスが検出されなかった場合は（ステップS107でNO）、ステップS106へ移行し処理を繰り返す。なお、ステップS105からステップS108の処理についての詳細は後述する。

## 【0046】

実行履歴を受信した中央装置1は感染時期を特定し（ステップS109）、また感染経路を特定する（ステップS1010）。なお、これらの処理の詳細についても後述する。そして感染時期、感染経路、検出したコンピュータウイルス名及び対処方法等の感染情報を端末装置2へ送信する（ステップS1011）。端末装置2は送信された感染情報を表示部24に表示する（ステップS1012）。図14は表示部24に表示された感染情報の内容を示す説明図である。図14に示すように、感染時期及び感染経路等の感染情報が表示部24に表示される。

## 【0047】

図15は端末装置2でのコンピュータウイルスチェックの手順を示すフローチャートである。まず、端末装置2は中央装置1から送信されたワクチンを記憶部25に登録し、また登録日時をも登録する（ステップS141）。そして端末装置2は、登録したワクチンを実行して、登録した日時以前について、ワクチンを実行する（ステップS142）。具体的には、記憶部25に記憶しているファイルをスキャンしパターンマッチングする。ここでコンピュータウイルスが検出されたか否かを判断する（ステップS143）。ここで、コンピュータウイルスが検出された場合は（ステップS143でYES）、実行履歴を実行履歴ファイル251に記憶した後（ステップS144）、記憶した実行履歴を読み出して実行履歴タイプAを中央装置1へ送信する（ステップS145）。なお、送信する情報としては端末装置2のアドレス、ワクチンの実行日時、検出したコンピュータウイルスに係るファイル名、該ファイルが更新された日時等を送信する。

## 【0048】

一方、コンピュータウイルスが検出されなかった場合（ステップS143でN

○)、実行履歴を実行履歴ファイル251に記憶する(ステップS146)。続いてワクチンがRAM常駐型か否かを判断する(ステップS147)。つまり、ワクチンにはRAM22に常駐して、ファイルが操作される度にコンピュータウィルスチェックを実行するRAM常駐型と、一定期間毎(例えば5時間毎)にワクチンを実行する非RAM常駐型とが存在する。RAM常駐型か否かによって感染時期の特定時期が左右されるため以下の如く処理を行う。

【0049】

ワクチンがRAM常駐型である場合は(ステップS147でYES)、ファイルの操作の度にコンピュータウィルスチェックを実行しコンピュータウィルスが検出されたか否かを判断する(ステップS148)。ここで、コンピュータウィルスが検出されなかった場合は(ステップS148でNO)、実行履歴ファイル251に実行履歴を記憶する(ステップS149)。その後、ステップS148へ移行し処理を繰り返す。一方、コンピュータウィルスが検出された場合は(ステップS148でYES)、実行履歴を実行履歴ファイル251に記憶した後(ステップS1410)、記憶した実行履歴を読み出して実行履歴タイプBを中央装置1へ送信する(ステップS1411)。

【0050】

一方、ワクチンが非RAM常駐型である場合は(ステップS147でNO)、一定期間毎にコンピュータウィルスチェックを実行し、コンピュータウィルスが検出されたか否かを判断する(ステップS1412)。ここで、コンピュータウィルスが検出されなかった場合は(ステップS1412でNO)、実行履歴ファイル251に実行履歴を記憶する(ステップS1413)。その後、ステップS1412へ移行し処理を繰り返す。一方、コンピュータウィルスが検出された場合は(ステップS1412でYES)、実行履歴を実行履歴ファイル251に記憶した後(ステップS1414)、記憶した実行履歴を読み出して実行履歴タイプCを中央装置1へ送信する(ステップS1415)。

【0051】

図16は感染時期及び感染経路を特定する際の処理手順を示すフローチャートである。端末装置2から送信された実行履歴タイプA乃至Cによって以下の処理

に分岐する。まず、送信された実行履歴がタイプAか否かを判断する（ステップS151）。タイプAである場合（ステップS151でYES）、感染時期をワクチン発見日時から端末装置2のワクチン登録日時までの間に特定する（ステップS152）。また感染経路を中央装置、他のISPまたは記録媒体と特定する（ステップS153）。すなわち、端末装置2においてワクチンが登録される以前に感染していることから、感染時期はワクチンの登録日時以前であることが特定でき、また中央装置1を備えるISPを経由して感染したことを否定できないことが理解できる。

#### 【0052】

送信された実行履歴がタイプAでない場合（ステップS151でNO）、送信された実行履歴がタイプBか否かを判断する（ステップS154）。タイプBである場合（ステップS154でYES）、すなわちワクチンがRAM常駐型である場合は、感染時期を、ワクチンを今回実行した日時に特定する（ステップS155）。すなわち、RAM常駐型はファイル操作時にリアルタイムでコンピュータウィルスのチェックを実行するため、感染時期を完全に特定することが可能である。また、感染経路を中央装置以外の他のISPまたは記録媒体と特定する（ステップS156）。すなわち、ステップS143において端末装置2にワクチンを登録した日時以前にはコンピュータウィルスが存在せず、かつワクチン登録後に検出されたことから、中央装置1に係るISP以外の他のISPまたは記録媒体経由で感染したことが特定できる。

#### 【0053】

送信された実行履歴がタイプBでない場合（ステップS154でNO）、すなわちワクチンが非RAM常駐型である場合は、感染時期を、ワクチンを前回に実行した日時から今回実行した日時の間に特定する（ステップS157）。すなわち、非RAM常駐型は一定期間毎にコンピュータウィルスのチェックを実行するため、実行履歴を参照すれば、前回実行日時から今回実行日時の間に感染したことが特定できる。また、感染経路を中央装置以外の他のISPまたは記録媒体と特定する（ステップS158）。すなわち、ステップS143において端末装置2にワクチンを登録した日時以前にはコンピュータウィルスが存在せず、かつワ



クチン登録後に検出されたことから、中央装置 1 に係る I S P 以外の他の I S P または記録媒体経由で感染したことが特定できる。

## 【 0 0 5 4 】

本実施の形態 2 は以上の如き構成としてあり、その他の構成及び作用は実施の形態 1 と同様であるので、対応する部分には同一の参照番号を付してその詳細な説明を省略する。

## 【 0 0 5 5 】

## 実施の形態 3

図 1 7 は実施の形態 3 に係る本発明の概要を示す模式図である。実施の形態 1 及び実施の形態 2 に係る中央装置 1 を実行させるためのコンピュータプログラムは、本実施の形態 3 のように中央装置 1 にプレインストールして提供することも、また C D - R O M 、 M O 等の可搬型記録媒体で提供することも可能である。さらに、コンピュータプログラムを回線経由で搬送波として伝搬させて提供することも可能である。以下に、その内容を説明する。

## 【 0 0 5 6 】

図 1 7 に示す中央装置 1 に、通信履歴を記憶させ、感染時期を特定させるプログラムが記録された記録媒体 1 a ( C D - R O M 、 M O 又は D V D - R O M 等) が中央装置 1 の記憶部 1 5 にインストールされている。かかるプログラムは中央装置 1 の R A M 1 2 にロードして実行される。これにより、上述のような本発明の中央装置 1 として機能する。

## 【 0 0 5 7 】

本実施の形態 3 は以上の如き構成としてあり、その他の構成及び作用は実施の形態 1 及び実施の形態 2 と同様であるので、対応する部分には同一の参照番号を付してその詳細な説明を省略する。

## 【 0 0 5 8 】

(付記 1) 端末装置と中央装置との間で送受信される情報に、コンピュータウイルスが存在するか否かを検出し、検出したコンピュータウイルスに関する感染情報を提供するコンピュータウイルス感染情報提供方法において、

前記中央装置に、コンピュータウイルスを検出及び駆除するワクチンを登録し

、また前記端末装置の通信履歴を記憶しておき、前記登録したワクチンにより、前記コンピュータウィルスが検出された場合に、前記記憶した通信履歴に基づいて、感染時期を特定し、

該特定した感染時期を含む感染情報を前記中央装置から前記端末装置へ送信し

前記端末装置により、前記送信された感染情報を表示する

ことを特徴とするコンピュータウィルス感染情報提供方法。

(付記 2) 端末装置と中央装置との間で送受信される情報に、コンピュータウィルスが存在するか否かを検出し、検出したコンピュータウィルスに関する感染情報を提供するコンピュータウィルス感染情報提供システムにおいて、

前記中央装置は、

コンピュータウィルスを検出及び駆除するワクチンを登録する手段と、

前記端末装置の通信履歴を記憶する手段と、

前記登録したワクチンにより、前記コンピュータウィルスが検出された場合に、前記記憶した通信履歴に基づいて、感染時期を特定する特定手段と、

前記特定した感染時期を含む感染情報を前記端末装置へ送信する感染情報送信手段と

を備え、

前記端末装置は、

前記送信された感染情報を表示する手段

を備えることを特徴とするコンピュータウィルス感染情報提供システム。

(付記 3) 前記中央装置は、

前記コンピュータウィルスが発見された発見日時を登録する手段

を更に備え、

前記特定手段は、

前記登録したワクチンにより、前記コンピュータウィルスが検出された場合に、前記記憶した通信履歴、前記登録した発見日時、及び前記ワクチンを登録したワクチン登録日時に基づいて、感染時期を特定するよう構成してある

ことを特徴とする付記 2 に記載のコンピュータウィルス感染情報提供システム

（付記 4） 前記中央装置は、  
前記記憶した通信履歴及び前記ワクチンを登録した登録日時に基づいて前記コンピュータウィルスの感染経路を特定する経路特定手段  
を更に備え、  
前記感染情報送信手段は、  
前記特定した感染経路、及び前記特定した感染時期を含む感染情報を前記端末装置へ送信するよう構成してあることを特徴とする付記 2 または 3 に記載のコンピュータウィルス感染情報提供システム。

（付記 5） 前記中央装置は、  
前記登録したワクチンを予め指定された端末装置へ送信する手段  
を更に備え、  
前記端末装置は、  
前記送信されたワクチンを登録する手段と、  
該登録したワクチンの実行履歴を記憶する手段と、  
前記ワクチンにより、前記コンピュータウィルスが検出された場合に、前記記憶した実行履歴を前記中央装置へ送信する実行結果送信手段  
を更に備え、  
前記中央装置は、  
前記実行結果送信手段により送信された実行履歴及び前記登録した発見日時に基づいて感染時期を特定する補助特定手段と、  
前記実行結果送信手段により送信された実行履歴に基づいて、前記コンピュータウィルスの感染経路を特定する補助経路特定手段と、  
前記補助特定手段により特定した感染時期、及び前記補助経路特定手段により特定した感染経路を含む感染情報を前記端末装置へ送信する手段と  
を更に備えることを特徴とする付記 3 または 4 に記載のコンピュータウィルス感染情報提供システム。

（付記 6） 前記ワクチンによりコンピュータウィルスが検出された場合に、該ワクチンの提供に関する案内情報を前記端末装置へ送信する手段

を更に備えることを特徴とする付記 2 乃至 4 のいずれかに記載のコンピュータウイルス感染情報提供システム。

(付記 7) 外部から送受信される情報にコンピュータウイルスが存在するか否かを検出し、検出したコンピュータウイルスに関する感染情報を提供する感染情報提供装置において、

コンピュータウイルスを検出及び駆除するワクチンを登録する手段と、

前記情報の通信履歴を記憶する手段と、

前記登録したワクチンにより、前記コンピュータウイルスが検出された場合に、前記記憶した通信履歴に基づいて、感染時期を特定する特定手段と、

前記特定した感染時期を含む感染情報を外部へ送信する感染情報送信手段とを備えることを特徴とする感染情報提供装置。

(付記 8) 前記コンピュータウイルスが発見された発見日時を登録する手段

を更に備え、

前記特定手段は、

前記登録したワクチンにより、前記コンピュータウイルスが検出された場合に、前記記憶した通信履歴、前記登録した発見日時、及び前記ワクチンを登録したワクチン登録日時に基づいて、感染時期を特定するよう構成してある

ことを特徴とする付記 7 に記載の感染情報提供装置。

(付記 9) 前記中央装置は、

前記記憶した通信履歴及び前記ワクチンを登録した登録日時に基づいて前記コンピュータウイルスの感染経路を特定する経路特定手段

を更に備え、

前記感染情報送信手段は、

前記特定した感染経路、及び前記特定した感染時期を含む感染情報を外部へ送信するよう構成してある

ことを特徴とする付記 7 または 8 に記載の感染情報提供装置。

(付記 10) 外部から送受信される情報にコンピュータウイルスが存在するか否かを検出し、検出したコンピュータウイルスに関する感染情報を提供させ

るコンピュータプログラムにおいて、

コンピュータに、前記情報の通信履歴を記憶させるステップと、

コンピュータに、コンピュータウィルスを検出及び駆除するワクチンにより、前記コンピュータウィルスが検出された場合に、前記記憶させた通信履歴に基づいて、感染時期を特定させる特定ステップと

を実行させることを特徴とするコンピュータプログラム。

(付記 1 1) 外部から送受信される情報にコンピュータウィルスが存在するか否かを検出し、検出したコンピュータウィルスに関する感染情報を提供させるコンピュータプログラムが記録されており、コンピュータでの読み取りが可能な記録媒体において、

コンピュータに、前記情報の通信履歴を記憶させるステップと、

コンピュータに、コンピュータウィルスを検出及び駆除するワクチンにより、前記コンピュータウィルスが検出された場合に、前記記憶させた通信履歴に基づいて、感染時期を特定させる特定ステップと

を実行させるためのコンピュータプログラムが記録されていることを特徴とするコンピュータでの読み取り可能な記録媒体。

【 0 0 5 9 】

【発明の効果】

以上詳述した如く、第 1 発明及び第 2 発明にあつては、中央装置にコンピュータウィルスを検出及び駆除するワクチンを登録しておく。また、中央装置は通信網を介して接続される端末装置が送信する情報の通信履歴を記憶する。そして、登録したワクチンにより、送信される情報中にコンピュータウィルスが検出された場合、記憶した通信履歴に基づいて、感染時期を特定する。そして、この特定した感染時期を含む感染情報を前記端末装置へ送信し、前記端末装置は、送信された感染時期を含む感染情報を表示するようにしたので、ユーザはより詳細なコンピュータウィルスの情報を入手でき、感染原因を特定することが容易となる。特に、係る詳細な感染情報を提供することで、他の I S P との差別化を図り、I S P の付加価値を飛躍的に高めることが可能となる。

【 0 0 6 0 】

第3発明にあつては、感染時期の特定に当たって、さらに、ワクチン製作会社、またはISPがコンピュータウィルスを最初に発見した日時を考慮する。すなわち、コンピュータウィルスは最初に発見されてから次第に蔓延していく性質を有することから、コンピュータウィルスが最初に発見される以前に、ユーザの端末装置がコンピュータウィルスに感染している場合は、極めて稀である。換言すれば感染時期が発見日時以前である可能性は極めて低い。

## 【0061】

また、感染時期の特定に当たって、さらに、発見されたコンピュータウィルスに対するワクチンを中央装置に登録した日時を考慮する。つまり、中央装置にワクチンを登録した登録日時以降は、完全に中央装置を経由するコンピュータウィルスはブロックすることが可能である。従って、コンピュータウィルスが検出された場合、前回の情報送信日時がワクチン登録日時以降であるか否かによって、感染時期が大きく異なる。前回の情報送信時がワクチン登録日時以降である場合は、前回はコンピュータウィルスに感染していることはあり得ないことから、前回情報を送信した日時から今回情報を送信した日時の間に、他のISP経由または記録媒体経由で感染したことが特定できる。一方、今回情報を送信し、コンピュータウィルスが検出された場合に、前回情報を送信した日時が、ワクチン登録日時以前である場合は、感染時期はそれ以前の発見日時から今回情報を送信した日時の間であることが特定できる。以上のように、感染時期を詳細に決定すべく判断要素として通信履歴に加えて、コンピュータウィルスの発見日時及びワクチン登録日時をも加えるようにしたので、より精度良く感染時期を特定でき、ユーザが感染原因を特定することがさらに容易になる。

## 【0062】

第4発明にあつては、記憶した通信履歴及びワクチンを登録した登録日時に基づいてコンピュータウィルスの感染経路を特定する。つまり、ワクチンを中央装置にインストールした後（登録日時の後）に、前回端末装置から情報を送信した場合にコンピュータウィルスが検出されず、今回情報を送信した場合に、コンピュータウィルスが検出されたということは、端末装置は明らかに中央装置（当該ISP）経由で感染したという可能性が無くなる。一方、ワクチンを中央装置に

インストールした後（登録日時の後）に、今回情報を送信した場合に、コンピュータウィルスが検出され、かつ前回情報を送信した日時が登録日時以前である場合は、登録日時以前に中央装置（当該ISP）を経由した可能性を否定できない。このように、通信履歴及びワクチンの登録日時に基づいてコンピュータウィルスの感染経路を特定し、感染経路をも感染情報としてユーザに提供することとしたので、ユーザはより感染経路を特定することが容易になる。

## 【0063】

第5発明にあっては、登録したワクチンを中央装置から予め指定された端末装置のみへ送信する。ワクチンが送信された端末装置は、ワクチンを登録する。そして、一定期間毎に、またはファイル操作時等に実行されるワクチンの実行履歴を記憶しておく。そして、ワクチンにより、コンピュータウィルスが検出された場合、前記記憶した実行履歴を中央装置へ送信する。

## 【0064】

中央装置は、実行履歴及び前記登録した発見日時に基づいて感染時期を特定する。また、送信された実行履歴に基づいて、コンピュータウィルスの感染経路を特定する。つまり上述した方法と同じく、ローカルな端末装置においてもウィルスチェックを行い、その実行履歴等の情報を回収し、これらに基づいて感染時期及び感染経路を特定して、ユーザへ提供する。従って、予め最新のワクチンの提供を受けるべくライセンス契約を行っているユーザは、新たなコンピュータウィルスの感染を防止することができる。また、ローカルな端末装置でのコンピュータウィルスチェックの結果に基づいて感染時期を特定しているので、さらに詳細に感染時期及び感染経路を特定することが可能となる。さらに、ISPの各ユーザから、ライセンス契約によりワクチンの製作に対する対価を確実に回収できることから、コンピュータウィルスの発生の度に、定期的な収入が見込め、ワクチン製作会社の経営基盤を盤石のものとすることが可能となる等、本発明は優れた効果を奏し得る。

## 【図面の簡単な説明】

## 【図1】

本発明に係るコンピュータウィルス感染情報提供システムの概要を示す模式図

である。

【図 2】

中央装置の構成を示すブロック図である。

【図 3】

ワクチン登録ファイルのレコードレイアウトを示す説明図である。

【図 4】

ユーザファイルのレコードレイアウトを示す説明図である。

【図 5】

通信履歴記憶ファイルのレコードレイアウトを示す説明図である。

【図 6】

本発明に係るコンピュータウイルス感染情報提供システムの処理手順を示すフローチャートである。

【図 7】

感染時期の特定処理及び感染経路の特定処理の手順を示すフローチャートである。

【図 8】

感染情報の表示例を示す説明図である。

【図 9】

実施の形態 2 に係るユーザファイルのレコードレイアウトを示す説明図である。

【図 1 0】

実施の形態 2 に係る端末装置の構成を示すブロック図である。

【図 1 1】

実行履歴ファイルの記録内容を示す説明図である。

【図 1 2】

実施の形態 2 に係るコンピュータウイルス感染情報提供システムの処理手順を示すフローチャートである。

【図 1 3】

案内情報のイメージを示す説明図である。



【図 1 4】

表示部に表示された感染情報の内容を示す説明図である。

【図 1 5】

端末装置でのコンピュータウイルスチェックの手順を示すフローチャートである。

【図 1 6】

感染時期及び感染経路を特定する際の処理手順を示すフローチャートである。

【図 1 7】

実施の形態 3 に係る本発明の概要を示す模式図である。

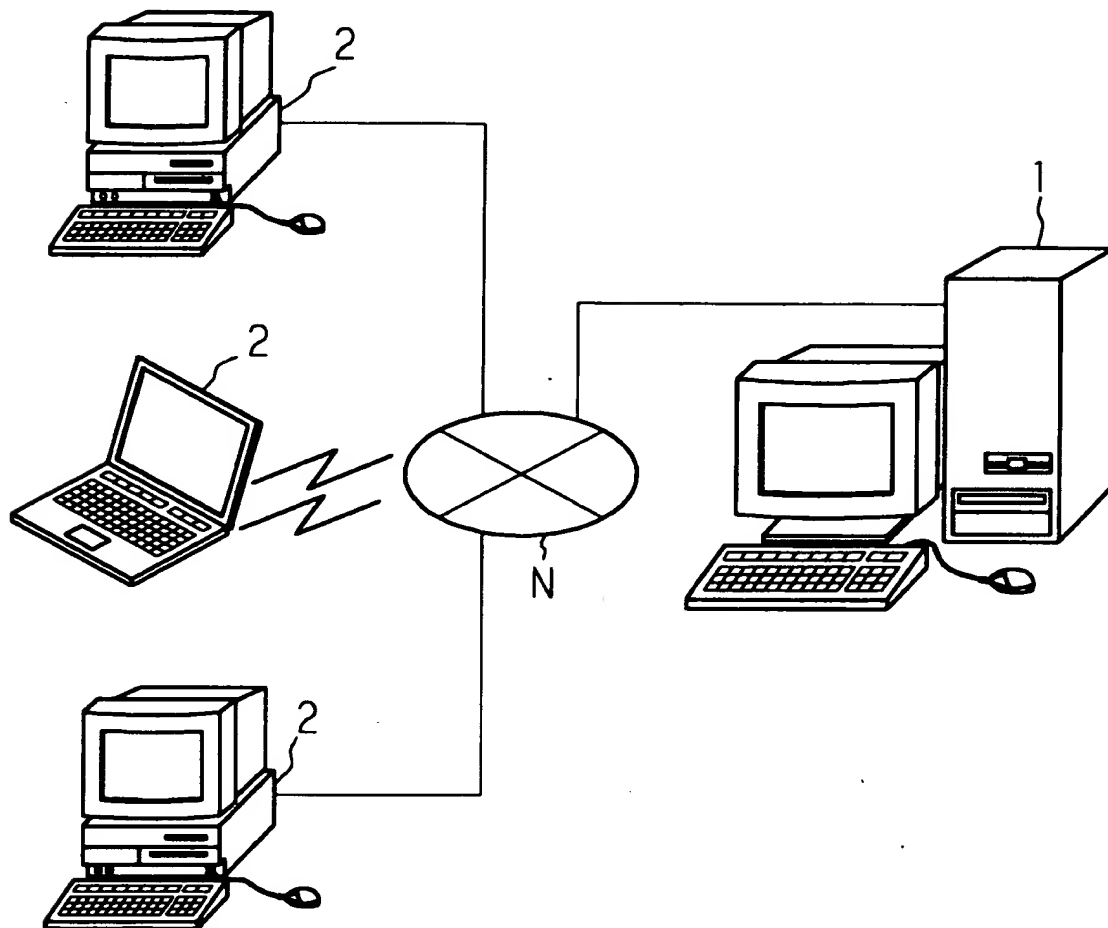
【符号の説明】

- 1 中央装置（感染情報提供装置）
  - 1 a 記録媒体
    - 1 5 1 ワクチン登録ファイル
    - 1 5 2 通信履歴記憶ファイル
    - 1 5 3 ユーザファイル
- 2 端末装置
  - 2 4 表示部
    - 2 5 1 実行履歴ファイル
- N 通信網

【書類名】 図面

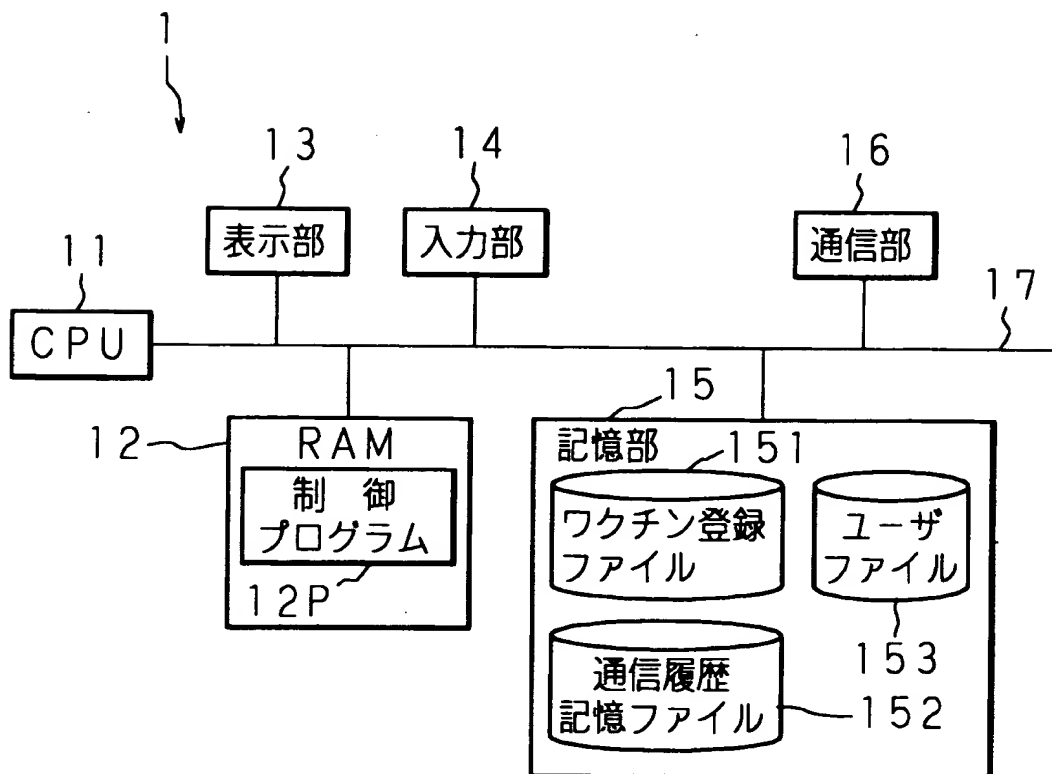
【図 1】

本発明に係るコンピュータウイルス感染情報提供システムの概要を示す模式図



【図 2】

中央装置の構成を示すブロック図



【図 3】

ワクチン登録ファイルのレコードレイアウトを示す説明図

151

ワクチンコード	コンピュータウイルス 発見日時	ワクチン登録日時
0001	2001/1/10	2001/1/14
0002	2001/1/30	2001/2/1
0003	2001/2/15	2001/2/18
⋮	⋮	⋮

【図 4】

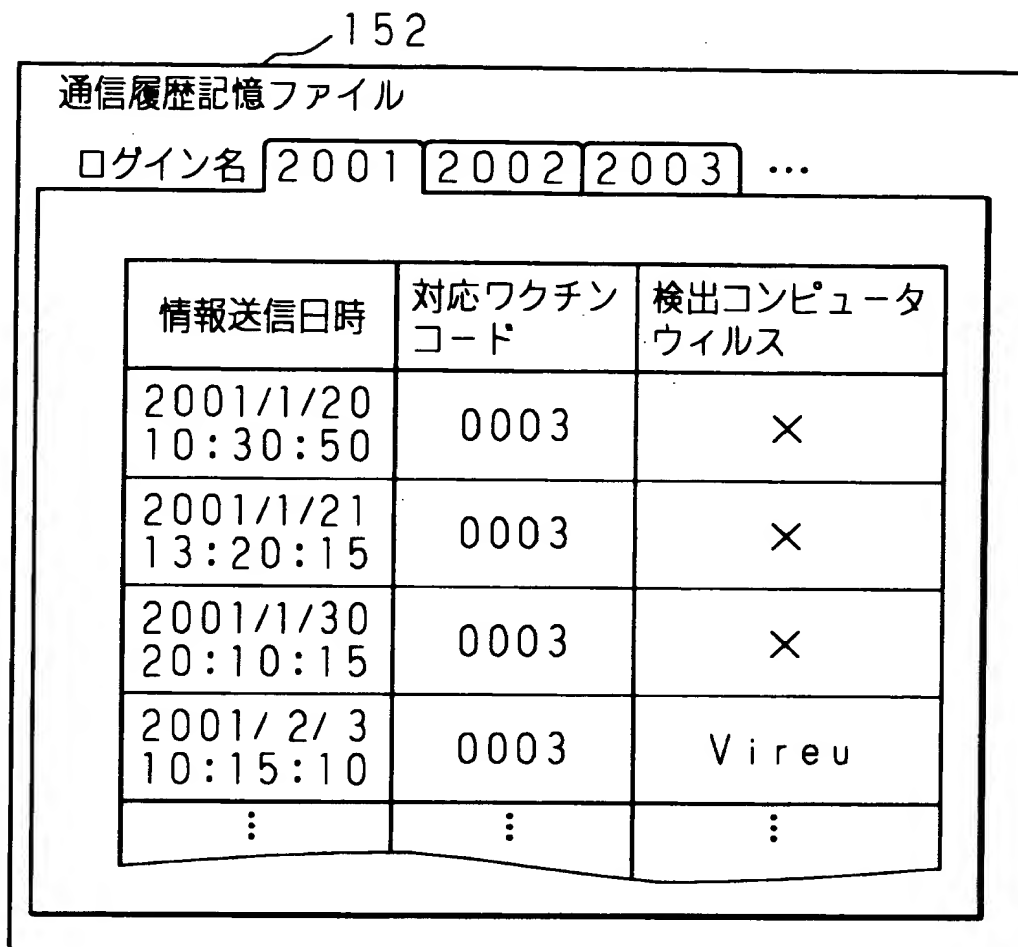
ユーザファイルのレコードレイアウトを示す説明図

153

ユーザファイル			
ログイン名	パスワード	電子メールアドレス	氏 名
2001	****	2001@ISP.com	○×△×
2002	****	2002@ISP.com	××△○
2003	****	2003@ISP.com	△△△△
⋮	⋮	⋮	⋮

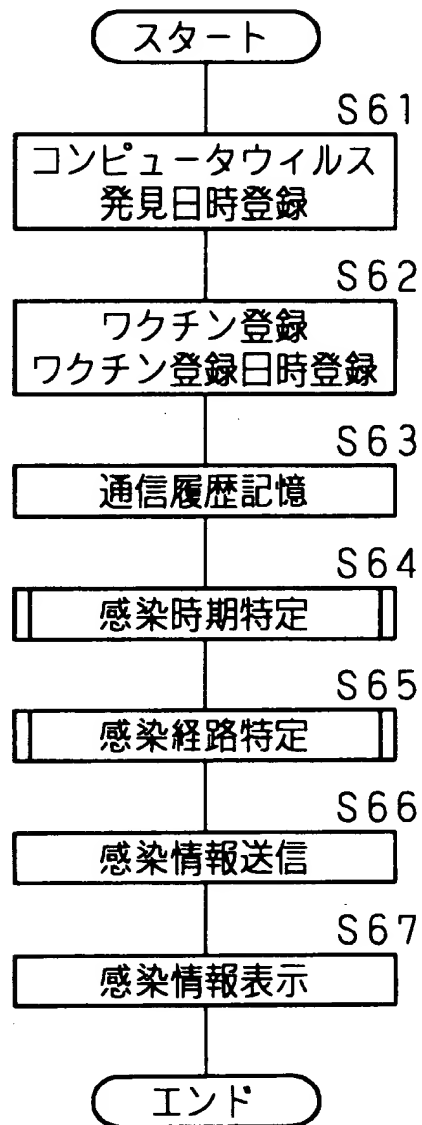
【図 5】

通信履歴記憶ファイルのレコードレイアウトを示す説明図



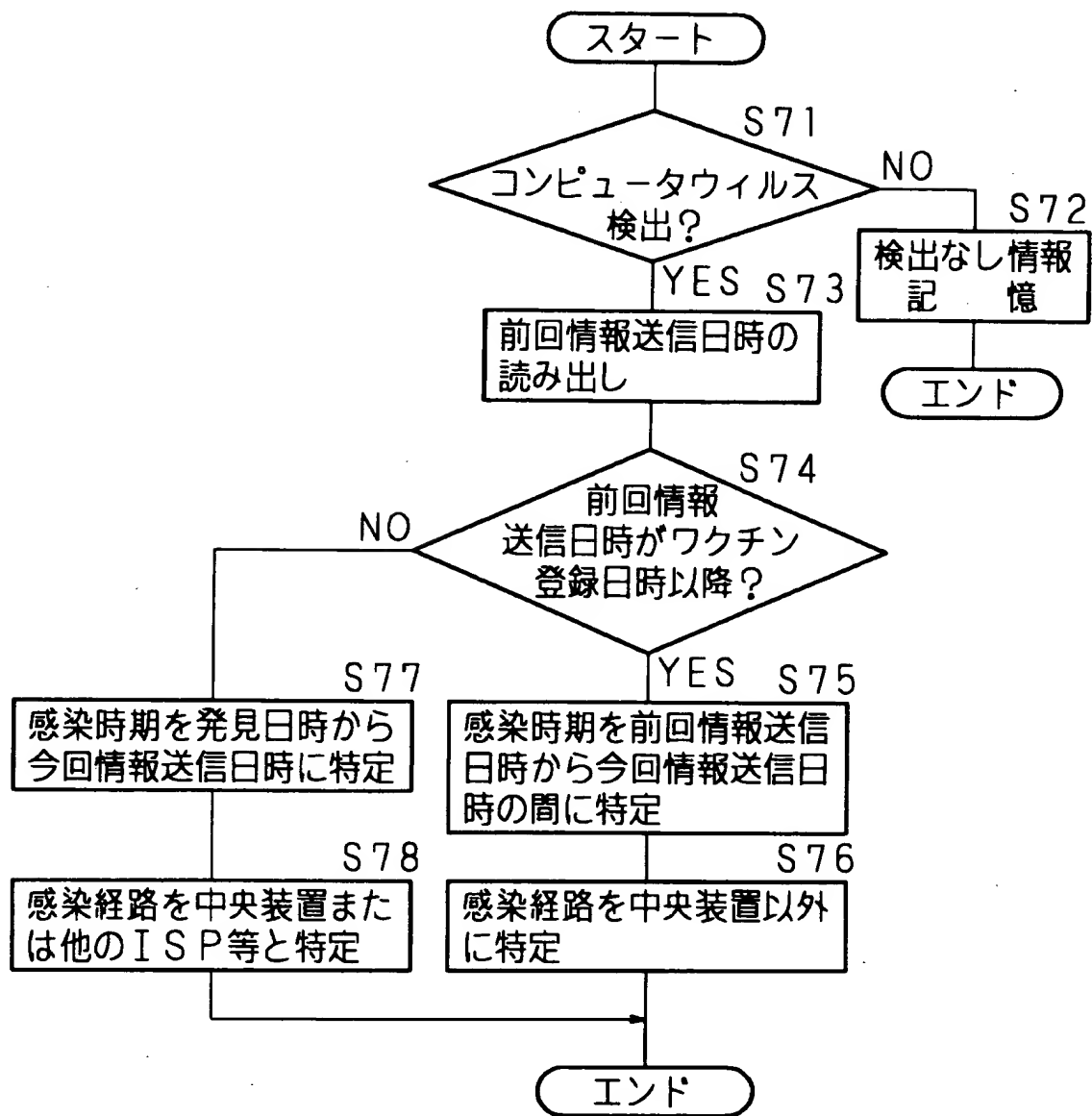
【図 6】

本発明に係るコンピュータウイルス感染情報提供システムの  
処理手順を示すフローチャート



【図 7】

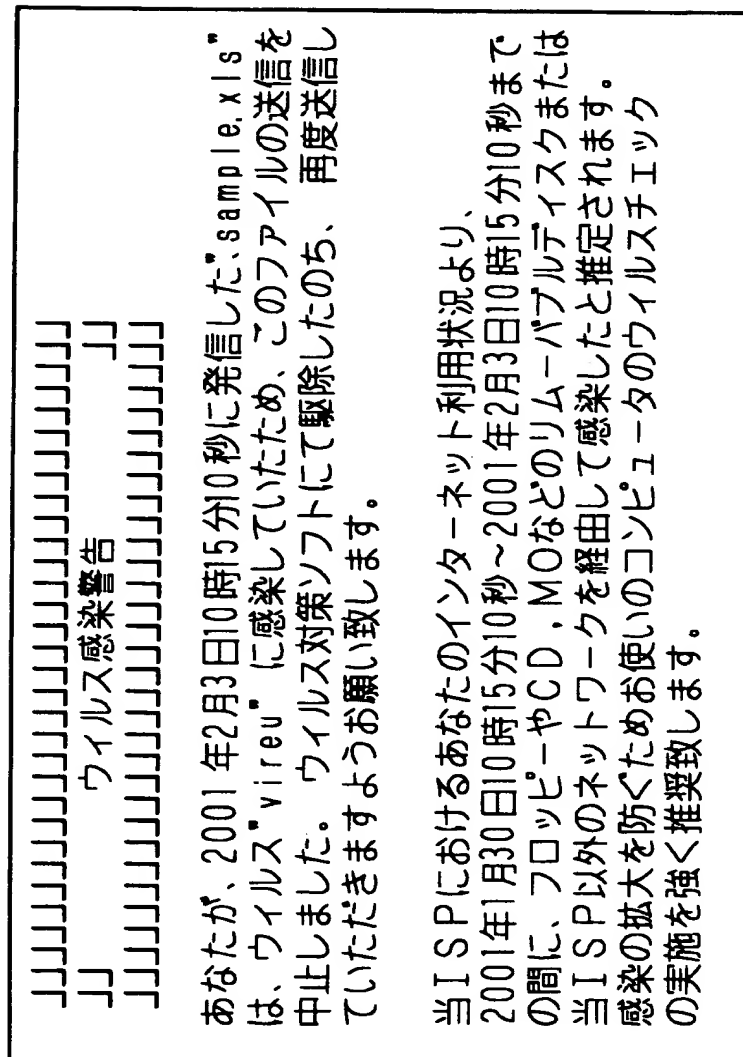
感染時期の特定処理及び感染経路の特定処理の  
手順を示すフローチャート





【図 8】

## 感染情報の表示例を示す説明図



【図 9】

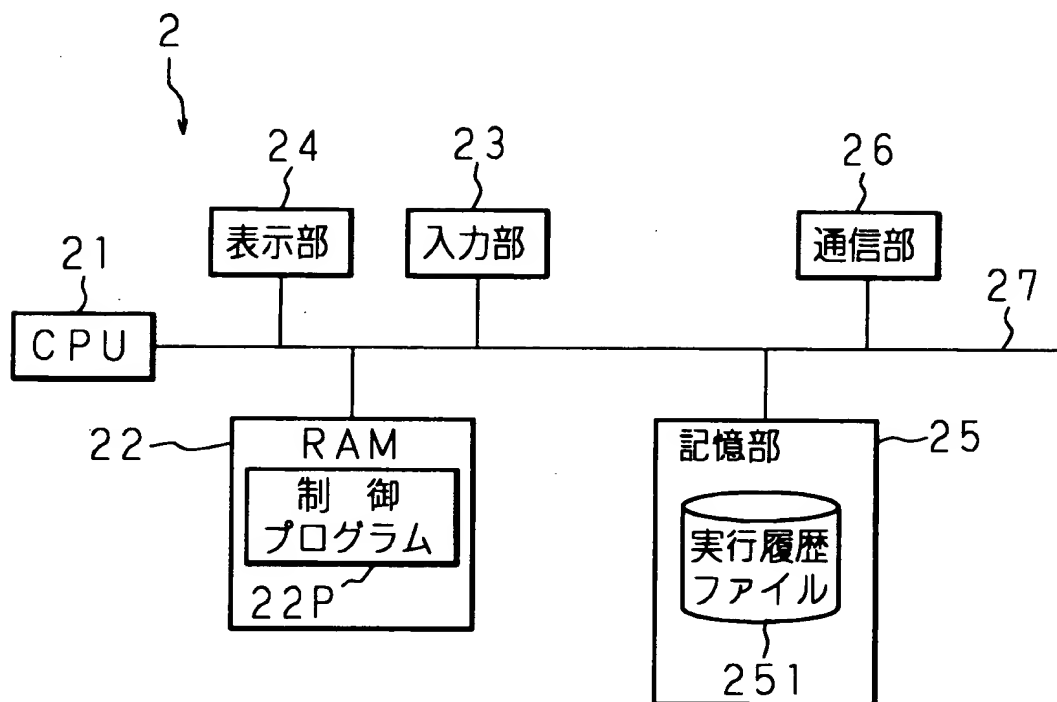
実施の形態 2 に係るユーザファイルの  
レコードレイアウトを示す説明図

ユーザファイル

ログイン名	パスワード	電子メールアドレス	氏 名	ワケチン登録
2001	*****	2001@ISP.com	OxΔx	O
2002	*****	2002@ISP.com	xxΔO	O
2003	*****	2003@ISP.com	ΔΔΔΔ	x
∴	∴	∴	∴	...

【図 1 0】

実施の形態 2 に係る端末装置の構成を示すブロック図



【図 1 1】

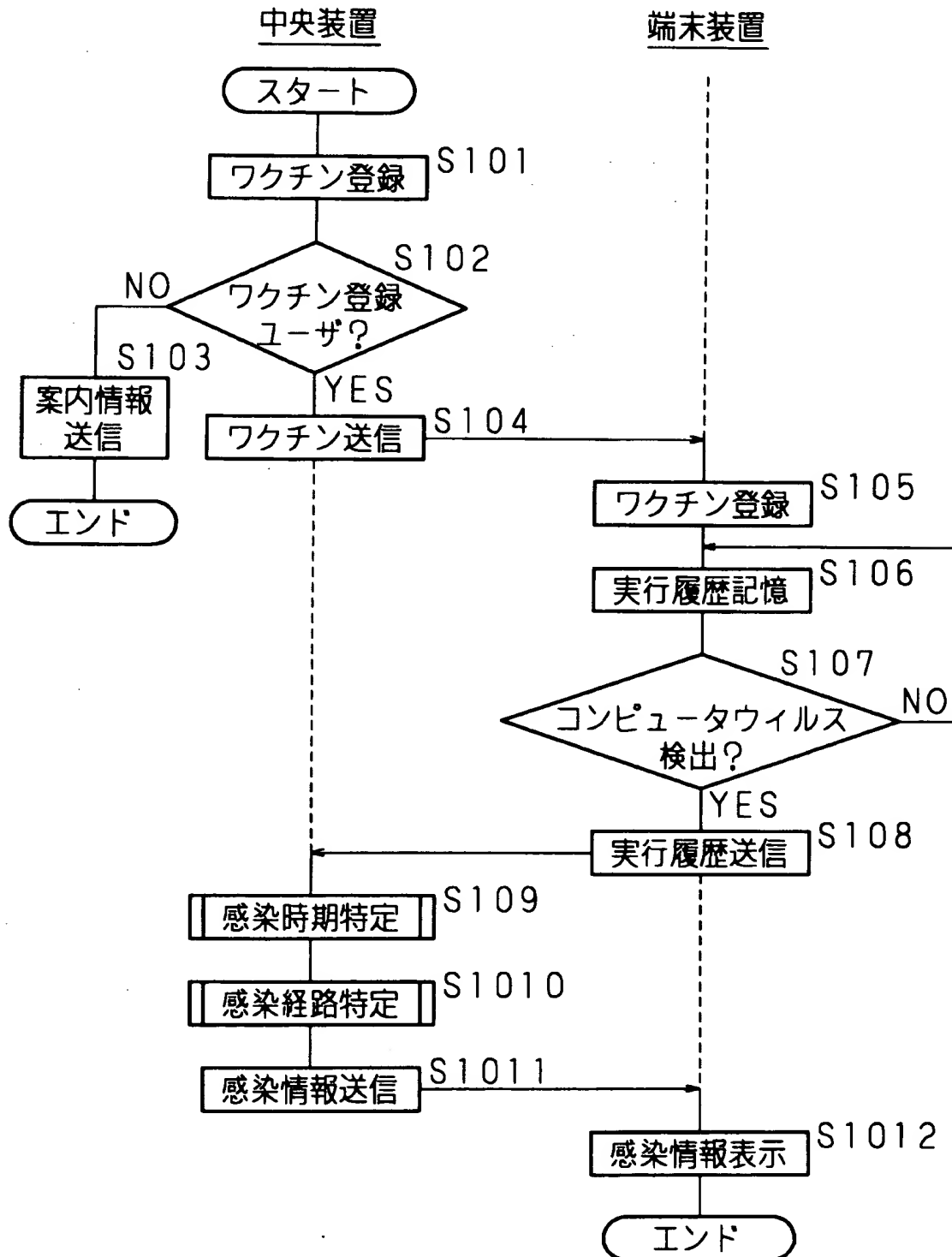
実行履歴ファイルの記録内容を示す説明図

251

実行履歴ファイル			
実行日時	検出結果	ワクチン コード	検出コンピュータ ウイルス
2001/ 1/ 2 12:25:13	×	0003	—
2001/ 1/ 5 16:10:35	×	0003	—
2001/ 1/ 7 2:10:15	×	0003	—
2001/1/15 12:12:45	○	0003	Vireu
⋮	⋮	⋮	⋮

【図 12】

実施の形態2に係るコンピュータウイルス感染情報提供システムの  
処理手順を示すフローチャート



【図 13】

## 案内情報のイメージを示す説明図

ウイルス感染警告

あなたが、2001年2月3日10時15分に発信した"sample.xls"は、ウイルス"vireu"に感染していたため、このファイルの送信を中止しました。ウイルス対策ソフトにて駆除したのち、再度送信していただきますようお願い致します。

当ISPにおけるあなたのインターネット利用状況より、  
2001年1月30日10時15分10秒～2001年2月3日10時15分10秒までの間に、フロッピーやCD、MOなどのリムーバブルディスクまたは当ISP以外のネットワークを経由して感染したと推定されます。  
感染の拡大を防ぐためお使いのコンピュータのウイルスチェックの実施を強く推奨致します。

お使いのコンピュータにより高い対ウイルス機能を望まれるなら、是非、当社でサポートしております。「ローカルウィルススキャン管理サービス」をお勧めします。当社ISPに接続することにより常に自動的に最新のウィルス情報が更新され、当社経由以外からの感染経路からも、あなたのコンピュータを守ります。

このサービスは付加サービスとしての追加料金がかかります。詳細はこちらをご覧ください。

【図 14】

表示部に表示された感染情報の内容を示す説明図

ウイルス検知報告

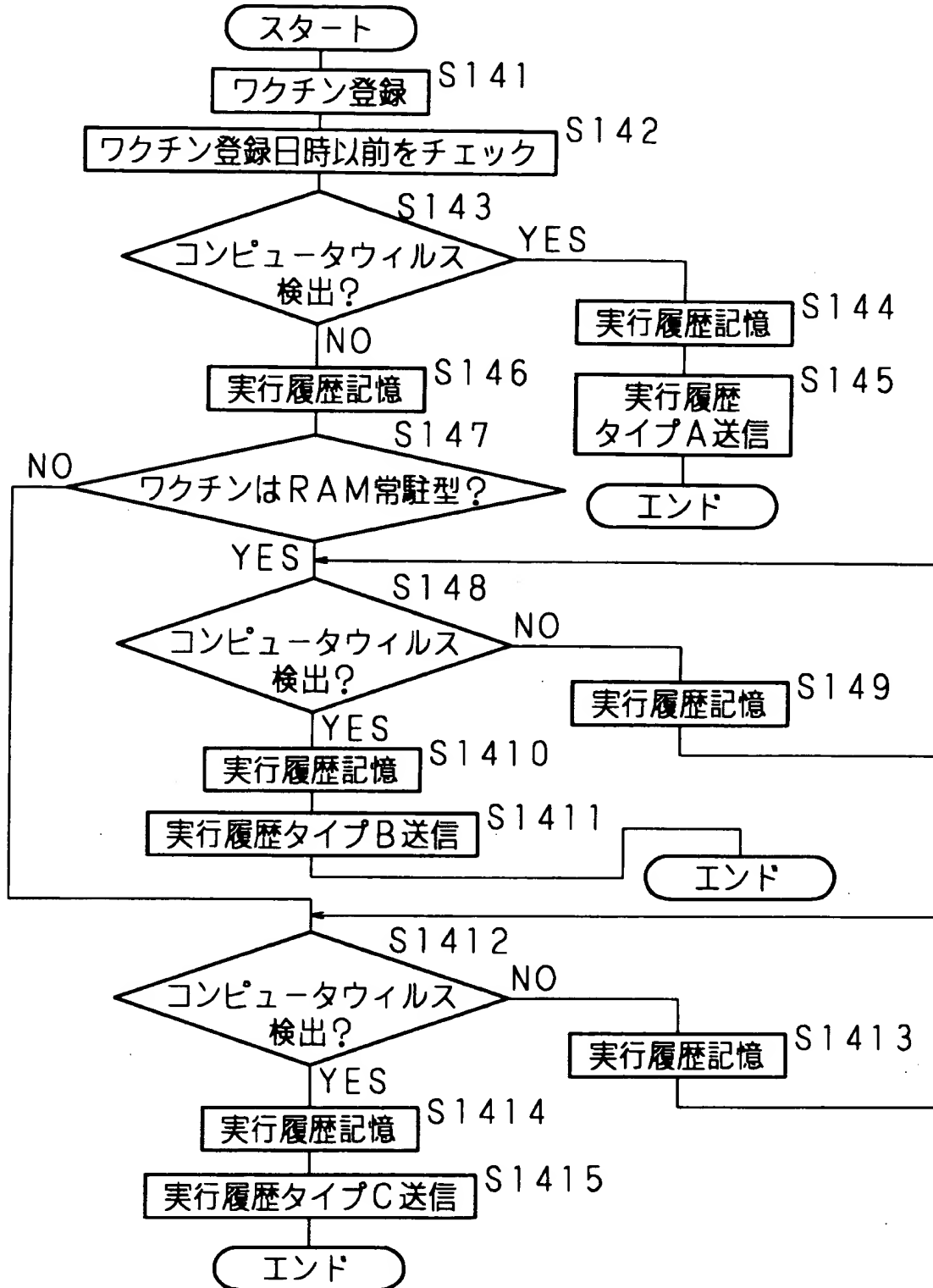
当社ウイルス監視システムにて、このコンピュータがウイルスに感染したことを検知したため、ただちに駆除いたしました。

当ISP側での駆除処理実施のため、下記のメールの送信が中止されましたので再送をお願いします。

このウィルスは“Virus”と呼ばれているもので、このコンピュータには、2001年1月7日2時10分15秒～2001年1月5日12時12分45秒までの間に、フロッピーやCD、MOなどのリムーバブルディスクまたは当ISP以外のネットワークを経由して感染したと推定されます。

---以下、 $\times$ -ル本文---

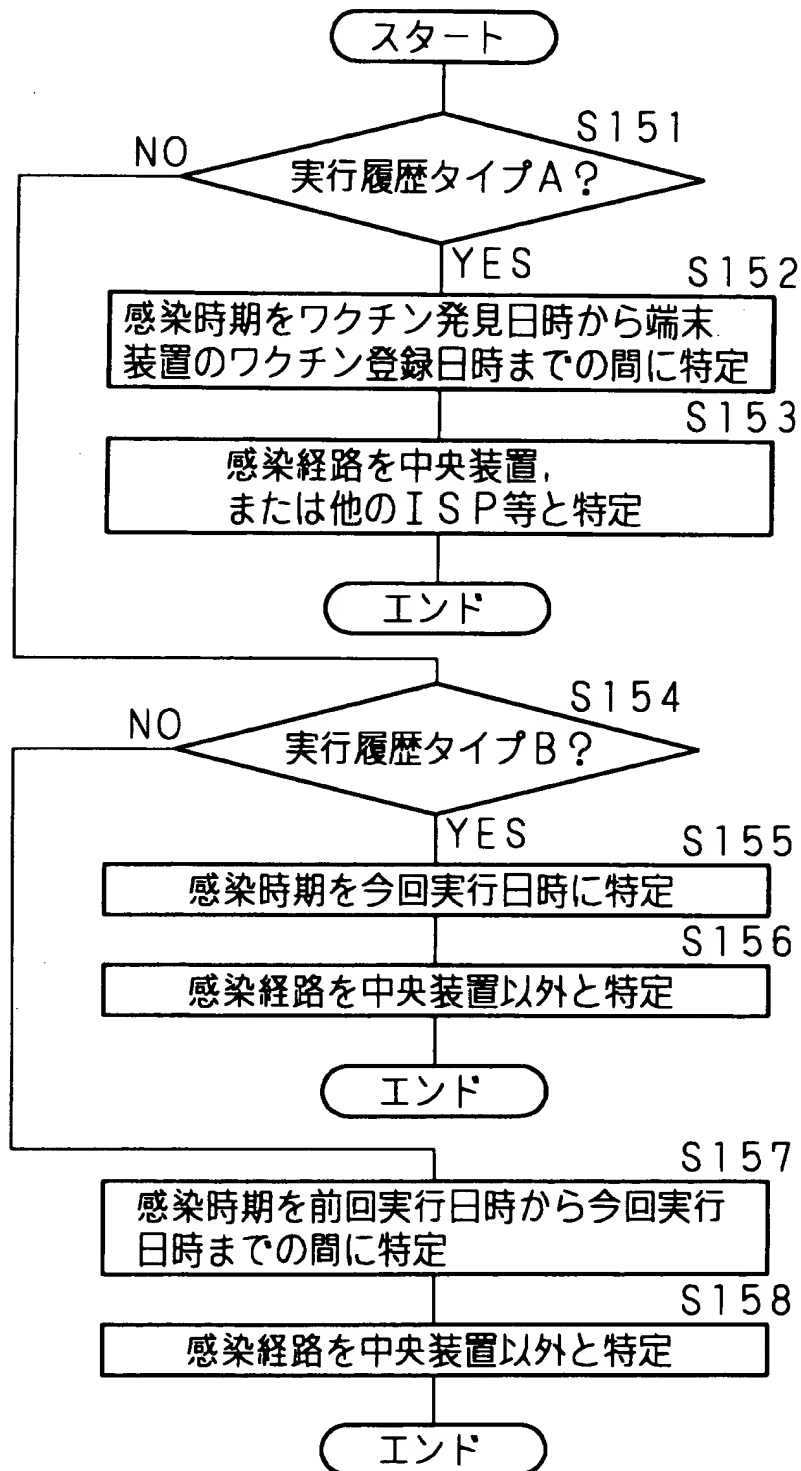
## 端末装置でのコンピュータウイルスチェックの手順を示すフローチャート





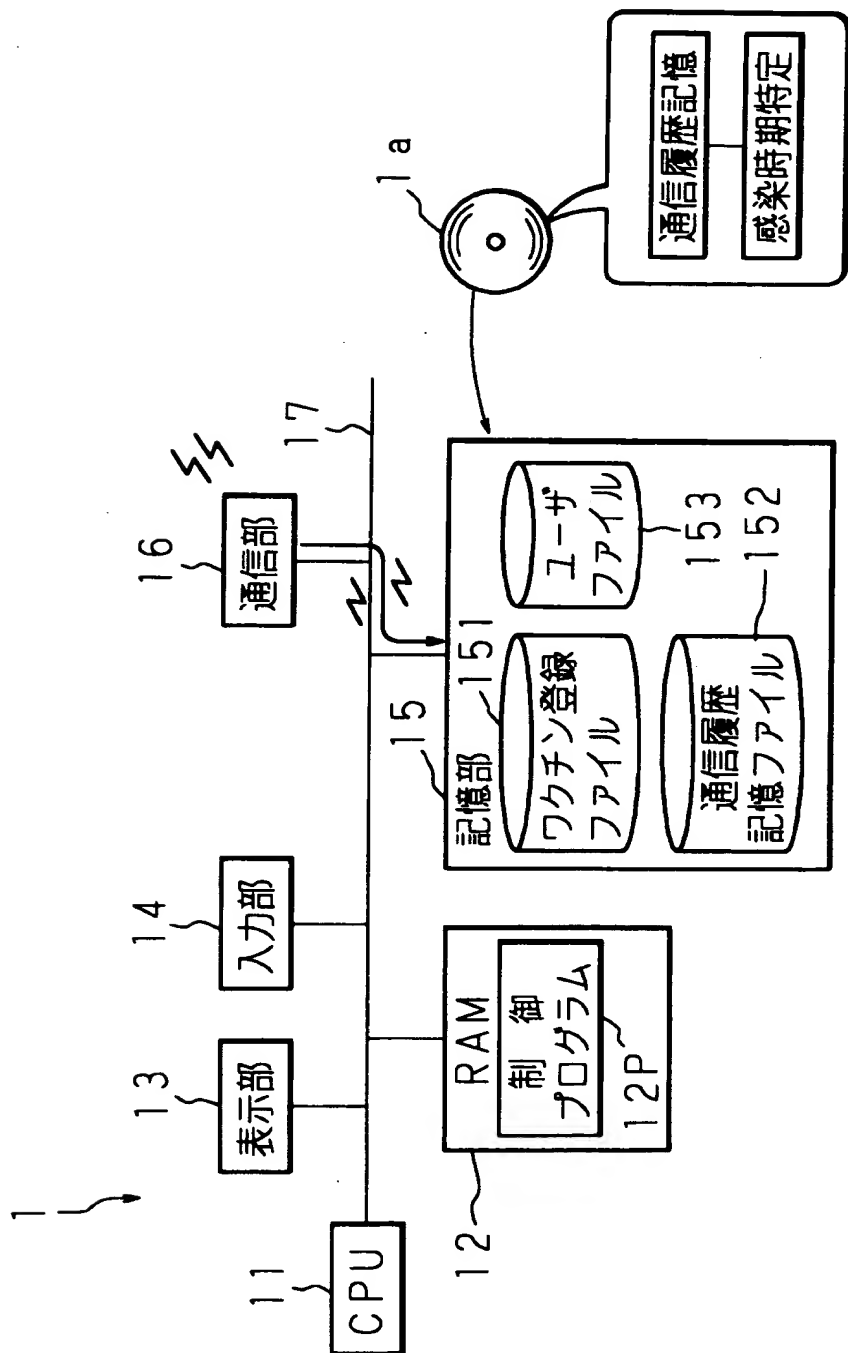
【図 16】

感染時期及び感染経路を特定する際の処理手順を示すフローチャート



【図 17】

実施の形態 3 に係る本発明の概要を示す模式図



【書類名】 要約書

【要約】

【課題】 感染時期等の感染情報をユーザに提供することにより、容易にユーザが感染時期を把握することができ、また I S P の付加価値を高めることが可能なコンピュータウィルス感染情報提供方法を提供する。

【解決手段】 中央装置にコンピュータウィルスを検出及び駆除するワクチンを登録しておく（ステップ S 6 2）。また、中央装置は端末装置が送信する情報の通信履歴を記憶する（ステップ S 6 3）。そして、登録したワクチンにより、送信される情報中にコンピュータウィルスが検出された場合、記憶した通信履歴に基づいて、感染時期を特定する（ステップ S 6 4）。そして、この特定した感染時期を含む感染情報を前記端末装置へ送信し（ステップ S 6 6）、前記端末装置は、送信された感染時期を含む感染情報を表示する（ステップ S 6 7）。

【選択図】 図 6

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社